

# Hudson's Theorem for finite-dimensional quantum systems

D. Gross

*Institute for Mathematical Sciences, Imperial College London, London SW7 2BW, UK and  
QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, UK \**

(Dated: February 1, 2008)

We show that, on a Hilbert space of odd dimension, the only pure states to possess a non-negative Wigner function are stabilizer states. The Clifford group is identified as the set of unitary operations which preserve positivity. The result can be seen as a discrete version of Hudson's Theorem. Hudson established that for continuous variable systems, the Wigner function of a pure state has no negative values if and only if the state is Gaussian. Turning to mixed states, it might be surmised that only convex combinations of stabilizer states give rise to non-negative Wigner distributions. We refute this conjecture by means of a counter-example. Further, we give an axiomatic characterization which completely fixes the definition of the Wigner function and compare two approaches to stabilizer states for Hilbert spaces of prime-power dimensions. In the course of the discussion, we derive explicit formulas for the number of stabilizer codes defined on such systems.

## I. INTRODUCTION

### A. General Introduction

The Wigner distribution establishes a correspondence between quantum mechanical states and real pseudo-probability distributions on phase space. 'Pseudo' refers to the fact that, while the Wigner function resembles many of the properties of probability distributions, it can take on negative values. This phenomenon has been linked to non-classical features of such quantum states (see Ref. [1] for an exposition of literature on that problem). It is naturally of interest to characterize those quantum states that are classical in the sense of giving rise to non-negative phase space distributions.

For the case of pure states described by vectors in  $\mathcal{H} = L^2(\mathbb{R})$ , the resolution of this problem was given by Hudson in Ref. [2]. Later, Soto and Claverie generalized Hudson's result to states of multi-particle systems (Ref. [3]).

**Theorem 1.** (Hudson, Soto, Claverie) *Let  $\psi \in L^2(\mathbb{R}^n)$  be a state vector. The Wigner function of  $\psi$  is non-negative if and only if  $\psi$  is a Gaussian state.*

*By definition, a vector is Gaussian if and only if it is of the form*

$$\psi(q) \propto e^{2\pi i(q\theta q + xq)},$$

where  $q, x \in \mathbb{R}^n$  and  $\theta$  is a symmetric matrix with entries in  $\mathbb{C}$  [40].

It is our objective to prove that the situation for discrete quantum systems is very similar, at least when the dimension of the Hilbert space is odd. Before stating the result, we pause for a brief overview of its main ingredients: discrete Wigner functions and stabilizer states.

The Wigner function [4] of a pure state  $\psi \in L^2(\mathbb{R})$  is computed as

$$W_\psi(p, q) = \pi^{-1} \int_{\xi \in \mathbb{R}} e^{-2\pi i \xi p} \bar{\psi}(q - \frac{1}{2}\xi) \psi(q + \frac{1}{2}\xi). \quad (1)$$

Equivalently,  $W_\psi$  is the (symplectic) Fourier transform of the characteristic function  $\Xi_\psi$ , which in turn is defined by

$$\Xi_\psi(p, q) = \text{tr}(w(p, q)^\dagger |\psi\rangle\langle\psi|).$$

Here,  $w(p, q) = e^{i(p\hat{X} - q\hat{P})}$  are the well-known Weyl or displacement operators [5, 6]. Partly triggered by the advent of quantum information theory, considerable work has been undertaken to explore Wigner functions for finite-dimensional quantum systems [7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. Two approaches might be identified in the literature on that subject. The first one aims to cast the definition of the Wigner function into a form that can be interpreted for both continuous variable and discrete systems [9, 10, 11, 15]. The second approach – introduced by Gibbons, Hoffman, and Wootters in Ref. [16] – focuses on the properties of Eq. (1). The authors imposed a set of axioms which a candidate definition of a discrete Wigner function would have to fulfill in order to resemble the well-known continuous counterpart.

We will argue that, for odd dimensions  $d$ ,

$$W_\psi(p, q) = d^{-1} \sum_{\xi \in \mathbb{Z}_d} e^{-\frac{2\pi i}{d} \xi p} \bar{\psi}(q - 2^{-1}\xi) \psi(q + 2^{-1}\xi)$$

is the most sensible analogue of Eq. (1), judged in terms of either of these approaches. Here,  $p, q$  are elements of  $\mathbb{Z}_d = \{0, \dots, d-1\}$  and  $2^{-1} = (d+1)/2$  is the multiplicative inverse of 2 modulo  $d$ . Indeed, the definition given above is the discrete symplectic Fourier transform of the discrete characteristic function and will be shown to be the *unique* choice to mimic certain desirable properties of the continuous Wigner function.

Stabilizer states were originally defined by Gottesman in Ref. [17] as the joint eigenvectors of certain sets of elements of the qubit Pauli group. Exceeding the case of qubits, stabilizer states for higher-dimensional quantum systems have been treated in the literature (see, e.g. Refs. [18, 19, 20, 21]). Such states find manifold applications in quantum information theory, ranging from quantum error correction [22] to Cluster state quantum computation [23]. Although displaying complex features such as multi-particle entanglement [24], stabilizer states allow for an efficient classical description. In particular, a quantum computer that operates only with stabilizer

\*Electronic address: davidg@qipc.org

states can offer no principal advantage over classical methods of computing [22]. The latter statement is sometimes called *Gottesman-Knill Theorem*.

Using that language, we intend to show:

**Theorem 2.** (Discrete Hudson's Theorem) *Let  $d$  be odd and  $\psi \in L^2(\mathbb{Z}_d^n)$  be a state vector. The Wigner function of  $\psi$  is non-negative if and only if  $\psi$  is a stabilizer state.*

*Given that  $\psi(q) \neq 0$  for all  $q$ , a vector  $\psi$  is a stabilizer state if and only if it is of the form*

$$\psi(q) \propto e^{\frac{2\pi}{d}i(q\theta q + xq)},$$

where  $q, x \in \mathbb{Z}_d^n$  and  $\theta$  is a symmetric matrix with entries in  $\mathbb{Z}_d$ .

Theorem 2 should convey two central messages. Firstly, if the right definitions are employed, the continuous and the discrete case behave very similarly (even though the methods of proof are completely different). Secondly, it adds further evidence to what might be called a piece of folk knowledge in the field of quantum information theory: namely that stabilizer states are the natural finite-dimensional analogue of Gaussian states.

The paper is organized as follows. We survey previous work on the subject in Section I B. Section II is devoted to a superficial, yet self-contained introduction to Weyl operators, characteristic functions, Wigner distributions and stabilizer states. The main theorem is proven in Section III. Sections V to VII address various related topics. The results of these last three sections do not rely on each other. Concretely, we comment on the relation between stabilizer states and Gaussian states in Section IV; we consider mixed states with positive Wigner functions in Section V and use Section VII for a discussion of Hilbert spaces whose dimension is the power of a prime.

Readers interested only in the structure of the proof, but not in its full generality, are deferred to Ref. [25], where a particularly simple special case of the main result is laid out.

## B. Previous Results

Recently, Galvao *et. al.* took a first step into the direction of classifying the quantum states with positive Wigner function [27]. To explain the relationship of their results to the present paper, we have to comment on an axiomatic approach to discrete Wigner functions and, further, on stabilizer states in dimensions that are the power of a prime number.

In Ref. [16], Gibbons, Hoffmann, and Wootters listed a set of requirements which should be met by any definition of a discrete Wigner function  $W$ . Denoting the dimension of the Hilbert space by  $d$ , their axioms amount to

1. (*Phase space*)  $W$  is a linear mapping sending operators to functions on a  $d \times d$  lattice, called the *phase space*.
2. (*Translational covariance*) The Wigner function is covariant under the action of the Weyl operators (in the sense of Theorem 7).

3. (*Marginal probabilities*) There exists a function  $Q(\lambda)$  that assigns a pure quantum state to every line  $\lambda$  in phase space. If  $\psi$  is state vector, then the sum of its Wigner function along  $\lambda$  must be equal to the overlap  $|\langle Q(\lambda) | \psi \rangle|^2$ .

Let us call functions that fall into this class *generalized Wigner functions*. This term is justified, as the characterization does not specify a unique solution: for a  $d$ -dimensional Hilbert space, there exist  $d^{d+1}$  distinct generalized Wigner functions. Note also that the construction has been described only for the case where  $d = p^n$  is the power of a prime, because only then the notion of a *line* in phase space has a well-defined meaning.

We turn to the second remark, concerning stabilizer states. Consider a composite system, built of  $n$   $d$ -level particles. We are free to conceive it as a single  $d^n$ -dimensional object. The two points of view give rise to different definitions of stabilizer states, the 'single-particle' one being starkly reduced as compared to the multiple-particle one. In Section VII, we show that the set of single-particle stabilizer states is strictly contained in the set of multi-particle ones. Indeed, the ratio of the respective cardinalities of the two sets grows super-exponentially in  $n$ . As an example, the generalized Bell and GHZ states

$$d^{-n/2} \sum_i |i\rangle \otimes |i\rangle, \quad d^{-n/2} \sum_i |i\rangle \otimes |i\rangle \otimes |i\rangle,$$

arguably the best-known multi-particle stabilizer states, do not belong to the respective single-particle sets.

The result of Ref. [27] concerns quantum states in prime-power dimensions that are non-negative with respect to *all* possible definitions of generalized Wigner functions. These states are shown to be mixtures of single-particle stabilizer states, as described above. The authors aim to establish necessary requirements for quantum computational speedup. Indeed, if the Wigner function of a quantum computer is positive at all times, then it operates only with stabilizer states and hence offers no advantage over classical computers, by the Gottesman-Knill Theorem.

Thus for the case of non-qubit pure states, Theorem 2 implies the results of Ref. [27] and goes further in two essential ways. Firstly, it suffices to look at a single definition of the Wigner function, as opposed to  $d^{n(d^n+1)}$  generalized ones. Secondly, quantum computation and the Gottesman-Knill Theorem are naturally set in the context of *multiple* particles. Our definition assigns positive Wigner functions to all multiple-particle stabilizer states, while Ref. [27] effectively relies on the single-particle definition [41]. On the other hand, our main theorem does not address qubits or mixed states, which Galvao *et. al.* do.

## II. PHASE SPACE FORMALISM

The term *phase space formalism* encompasses the ideas and tools in relation to the *Weyl representation*, to be defined shortly. We will give a concise introduction in this section. Many of the results presented can be found in the literature,

but some, e.g. the Clifford covariance of the Wigner function in non-prime dimensions, seem to be new.

### A. Weyl representation

We start by considering a  $d$ -dimensional quantum system,  $d$  odd. In its Hilbert space  $\mathcal{H}$ , we choose a basis  $\{|0\rangle, \dots, |d-1\rangle\}$ , labeled by elements of  $\mathbb{Z}_d$ . Henceforth,  $\mathbb{Z}_d$  will be referred to as the *configuration space* and abbreviated by  $Q$ .

The pivotal objects in the phase space formalism are the *Weyl operators* (also known as the *generalized Pauli operators*), as constructed below. Let  $\chi(q) = e^{\frac{2\pi}{d}iq}$ . The relations

$$\hat{x}(q)|x\rangle = |x+q\rangle, \quad \hat{z}(p)|x\rangle = \chi(px)|x\rangle \quad (2)$$

define the *shift* and *boost* operators respectively. The Weyl operators are given by

$$w(p, q) = \chi(-2^{-1}pq) \hat{z}(p) \hat{x}(q), \quad (3)$$

for  $p, q, t \in Q$ . The specific choice of phases will prove useful later on [42]. The set of Weyl operators is closed under multiplication, up to phase factors. Direct computation shows that the composition law is given by

$$\begin{aligned} & w(p, q)w(p', q') \\ &= \chi(2^{-1} \left[ \begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} p' \\ q' \end{pmatrix} \right]) w(p+p', q+q'). \end{aligned} \quad (4)$$

The square brackets denote the standard *symplectic inner product* on  $\mathbb{Z}_d^2$ :

$$\left[ \begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} p' \\ q' \end{pmatrix} \right] := \begin{pmatrix} p \\ q \end{pmatrix}^T J \begin{pmatrix} p' \\ q' \end{pmatrix} \quad (5)$$

where

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (6)$$

We write  $w(v) = w(v_p, v_q)$  for elements  $v = (v_p, v_q) \in \mathbb{Z}_d^2$ . The space  $V := Q \times Q$  with inner product given by Eq. (5) will be called *phase space* in the sequel, owing to its analogy to the phase space known in classical mechanics.

The preceding constructing generalizes naturally to multiple particles. Indeed, the configuration space of an  $n$ -particle system is given by  $Q = \mathbb{Z}_d^n$ . Multiplication between two elements  $p, q \in Q$  is understood as the usual inner product  $pq = \sum_i p_i q_i$ . The Hilbert space is again spanned by  $\{|q\rangle\}_{q \in Q}$  and the Weyl operators are defined to be the tensor products

$$\begin{aligned} w(p, q) &= w(p_1, \dots, p_n, q_1, \dots, q_n) \\ &= w(p_1, q_1) \otimes \dots \otimes w(p_n, q_n). \end{aligned} \quad (7)$$

Equations (4), (5) remain valid in the multiple-particle setting, if we substitute the matrix  $J$  by its multi-dimensional version

$$J = \begin{pmatrix} 0_{n \times n} & \mathbb{1}_{n \times n} \\ -\mathbb{1}_{n \times n} & 0_{n \times n} \end{pmatrix}.$$

We end this section with some miscellaneous remarks.

A state vector  $|\psi\rangle$  can be identified with a complex function on configuration space by setting  $\psi(q) = \langle q|\psi\rangle$ . We will use both representations interchangeably.

The continuous Weyl operators  $w(p, q) = e^{i(p\hat{X}-q\hat{P})}$ ,  $p, q \in \mathbb{R}$  fulfill exactly the same composition law as stated in Eq. (4), if  $\chi$  is set to  $\chi(q) = e^{iq}$  and the other symbols are interpreted in the obvious way. In fact, Eq. (4) is then equivalent to the fundamental *Weyl commutation relations* [6]. Having this analogy in mind,  $p$  and  $q$  will sometimes be called *momentum* and *position* coordinates respectively.

For future reference, note the two simple relations

$$(w(p, q)\psi)(x) = \chi(-2^{-1}pq + px)\psi(x - q), \quad (8)$$

$$\text{tr } w(p, q) = d^n \delta_{p,0} \delta_{q,0}. \quad (9)$$

It remains yet to justify the name *Weyl representation*. For  $v \in V, t \in \mathbb{Z}_d$ , define  $w(v, t) = \chi(t)w(v)$ . Equation (4) takes on the form

$$w(v_1, t_1)w(v_2, t_2) = w(v_1 + v_2, t_1 + t_2 + 2^{-1}[v_1, v_2]).$$

The set  $V \times \mathbb{Z}_d$ , equipped with the above composition law is called the *Heisenberg group*  $H(\mathbb{Z}_d^n)$ , the Weyl matrices constituting a unitary representation of  $H(\mathbb{Z}_d^n)$  [6]. This point of view on Weyl operators will be needed only in Appendix IX A.

### B. Clifford group

The Clifford group is the subset of the unitary operators that map Weyl operators to multiples of Weyl operators under conjugation:

$$Uw(v)U^\dagger = c(v)w(S(v)) \quad (10)$$

for some maps  $c : V \rightarrow \mathbb{C}$  and  $S : V \rightarrow V$  [17]. The structure of the Clifford group is described in the following theorem [43].

Before stating the theorem, we have to comment on a re-appearing issue: namely that things are more involved if  $d$  is not a prime number. For prime values of  $d$ ,  $\mathbb{Z}_d$  has the structure of a *finite algebraic field*,  $\mathbb{Z}_d^n$  is a *finite vector space* and most of the intuitions we have about vector spaces continue to be true. Among the more severe deficiencies of the general case is the fact that not every element  $a$  of  $\mathbb{Z}_d$  possesses a multiplicative inverse modulo  $d$ . But even if the analogue of a theorem about vector spaces holds for non-prime values of  $d$ , it is often difficult to find a proof in the literature. Appendices IX C and IX D contain a collection of statements of this kind. Less technically inclined readers will not loose much by skipping these sections.

For the sake of clarity of language, we call functions  $f$  on  $Q$  which fulfill  $f(\lambda a + b) = \lambda f(a) + f(b)$  *linear*, disregarding the fact that  $Q$  might fail to be a linear space. Similarly, a subset  $S$  of  $Q$  that is closed under addition and multiplication by elements of  $\mathbb{Z}_d$  is referred to as a *subspace*. We define a function  $S$  to be *symplectic* if it is linear and preserves the symplectic form:  $[S \cdot, S \cdot] = [\cdot, \cdot]$ .

**Theorem 3.** (Structure of the Clifford group)

1. For any symplectic  $S$ , there is a unitary operator  $\mu(S)$  such that

$$\mu(S) w(v) \mu(S)^\dagger = w(Sv).$$

2.  $\mu$  is a projective representation of the symplectic group, that is

$$\mu(S)\mu(T) = e^{i\phi} \mu(ST)$$

for some phase factor  $e^{i\phi}$ .

3. Up to a phase, any Clifford operation is of the form

$$U = w(a)\mu(S)$$

for a suitable  $a \in V$  and symplectic  $S$ .

The representation  $\mu$  is called the *Weil* or *metaplectic* representation [6, 28]. Theorem 3 could be called a discrete version of the celebrated *Stone-von Neumann Theorem* [6]. Its proof is not essential for understanding the further argument and has therefore been moved to Appendix IX A.

Note that a Clifford operation is connected to a vector  $a$  and a linear mapping  $S$ . This should remind us of a well-known structure on linear spaces: *affine transformations*. An affine mapping  $A$  is of the form  $A(b) = Sb + a$  where  $S$  is an invertible linear operator and  $a$  a vector. Let us call  $A$  symplectic if its linear part  $S$  is.

We will frequently use the 'dot notation' to define functions of one parameter; for example writing  $S \cdot + a$  for  $A$ .

**Lemma 4.** (Clifford group and affine transformations) *The mapping*

$$S \cdot + a \mapsto w(a)\mu(S)$$

*is a projective representation of the group of symplectic affine transformations.*

*Proof.* All we need to do is to compare the composition law of the affine group

$$\begin{aligned} (S \cdot + a) \circ (T \cdot + b) &= S(T \cdot + b) + a \\ &= ST \cdot + (Sb + a) \end{aligned}$$

to the composition law of the representation

$$\begin{aligned} w(a)\mu(S) w(b)\mu(T) &= w(a) \mu(S) w(b)\mu(S)^\dagger \mu(S)\mu(T) \\ &= w(a)w(Sb)\mu(S)\mu(T) \\ &\propto w(Sb + a)\mu(ST) \end{aligned}$$

which proves the assertion.  $\square$

The correspondence established by the last lemma will find a very tangible manifestation in Section IID, when we will see that the Clifford group induces affine transformations of the Wigner function.

### C. Fourier Transforms

Let  $Q = \mathbb{Z}_d^n$  and  $f : Q \rightarrow \mathbb{C}$  be a complex function on  $Q$ . The Fourier transform of  $f$  is

$$(\mathcal{F}f)(p) = \hat{f}(p) = |Q|^{-1/2} \sum_{q \in Q} \bar{\chi}(pq) f(q). \quad (11)$$

In the course of the main proof we will be confronted with Fourier transforms of functions which are defined only on a subspace of  $Q$ . If  $d$  is prime, then any subspace of  $Q = \mathbb{Z}_d^n$  is of the form  $\mathbb{Z}_d^{n'}$ , for some  $n' \leq n$ , so no new situation arises.

For non-prime dimensions, however, subspaces may not be as well-behaved. Consider as an example  $\{0, 3, 6\} \subset \mathbb{Z}_9^1$ . The set is closed under addition and multiplication, but can clearly not be written as  $\mathbb{Z}_9^{n'}$ .

To cope with this problem, we will cast Eq. (11) into a form that is well-defined for functions  $f$  on more general spaces. The construction is presented below. It can be found in any textbook on harmonic analysis (e.g. Ref. [29]).

A *character* of  $Q$  is a function  $\zeta : Q \rightarrow \mathbb{C}$  such that  $\zeta(a+b) = \zeta(a)\zeta(b)$ . Any character of  $Q$  is of the form  $\zeta(q) = \bar{\chi}(xq)$  for an appropriate  $x \in Q$  (see Appendix IX C). We can hence conceive the Fourier transformation defined in Eq. (11) as a function of the characters of  $Q$ :

$$\hat{f}(\zeta) = |Q|^{-1/2} \sum_q \zeta(q) f(q). \quad (12)$$

We denote the set of characters of  $Q$  by  $Q^*$ . With these notions, Eq. (12) defines a function  $Q^* \rightarrow \mathbb{C}$ . If, now,  $S$  is any subspace of  $Q$  and  $f$  a function on  $S$ , the Fourier transform

$$\hat{f} : S^* \rightarrow S \quad \hat{f}(\zeta) = |S|^{-1/2} \sum_s \zeta(s) f(s)$$

is well-defined.

For  $f : V \rightarrow \mathbb{C}$ , we define the *symplectic Fourier transform* as

$$(\mathcal{F}_S f)(a) = |V|^{-1/2} \sum_{b \in V} \bar{\chi}([a, b]) f(b). \quad (13)$$

Finally, take a note that the normalization in Eqs. (11) and (12) has been chosen in such a way that *Parseval's Theorem*  $\|f\| = \|\hat{f}\|$  holds, where  $\|f\|^2 = \sum_q |f(q)|^2$ .

### D. Definition and properties of the Wigner function

Employing Eq. (9) in conjunction with the composition law Eq. (4), one finds that the Weyl operators  $\{w(p, q)\}$  form an orthonormal basis in the space of operators on  $\mathcal{H}$  with respect to the trace scalar product  $d^{-n} \text{tr}(\cdot^\dagger \cdot)$ . The *characteristic function*  $\Xi_\rho$  of an operator  $\rho$  is given by its expansion coefficients with respect to the Weyl basis:

$$\Xi_\rho(\xi, x) = d^{-n} \text{tr}(w(\xi, x)^\dagger \rho). \quad (14)$$

We mentioned in the introduction that the continuous Wigner function is the symplectic Fourier transform of the characteristic function [5, 6]. The two latter concepts have been defined for finite-dimensional systems in the preceding paragraphs. We can now state, in complete analogy to the continuous case:

**Definition 5.** (Wigner function) *Let  $d$  be odd,  $Q = \mathbb{Z}_d^n$  for some  $n$ . Let  $V, \mathcal{H}$  be as usual and let  $\rho$  be a quantum state on  $\mathcal{H}$ .*

*The Wigner function  $W_\rho$  associated with  $\rho$  is the symplectic Fourier transformation of the characteristic function  $\Xi_\rho$ .*

An explicit calculation yields, for all  $a \in V$ ,

$$\begin{aligned} (\mathcal{F}_S \Xi_\rho)(a) &= d^{-2n} \sum_{b \in V} \bar{\chi}([a, b]) \operatorname{tr}(w(b)^\dagger \rho) \\ &= d^{-n} \operatorname{tr} \left( \left( d^{-n} \sum_b \bar{\chi}([a, b]) w(b)^\dagger \right) \rho \right) \\ &=: d^{-n} \operatorname{tr}(A(a) \rho), \end{aligned} \quad (15)$$

where we have implicitly defined the *phase space point operator*  $A(a)$  [16].

Theorem 6 lists a selection of properties of the Wigner function. For a more thorough discussion, the reader is deferred to Refs. [9, 15].

**Theorem 6.** (Properties of the Wigner function)

1. *The phase space point operators have unit trace and form an orthonormal basis in the space of Hermitian operators on  $\mathcal{H}$ . Hence the Wigner function of an Hermitian operator is real, and further, the overlap*

$$d^{-n} \operatorname{tr}(\rho \sigma) = \sum_{v \in V} W_\rho(v) W_\sigma(v),$$

*and normalization relations*

$$\sum_v W_\rho(v) = \operatorname{tr} \rho$$

*hold.*

2. *For a pure state  $\psi$ , the Wigner function  $W_\psi := W_{|\psi\rangle\langle\psi|}$  equals*

$$\begin{aligned} W_\psi(p, q) &= \\ d^{-n} \sum_{\xi \in Q} \bar{\chi}(\xi p) \bar{\psi}(q - 2^{-1}\xi) \psi(q + 2^{-1}\xi). \end{aligned}$$

3. *When computing marginal probabilities, the Wigner function behaves like a classical probability distribution:*

$$\sum_{p \in Q} W_\psi(p, q) = |\psi(q)|^2.$$

4. *The multi-particle phase space point operators factor:*

$$A(p_1, \dots, p_n, q_1, \dots, q_n) = \bigotimes_i^n A^{(i)}(p_i, q_i)$$

*(and hence so does the Wigner function).*

5. *It holds that  $A(0)|q\rangle = |-q\rangle$ . In other words, the phase space point operator at the origin equals the parity operator.*

6. *The Wigner function  $W_{\rho\sigma}$  of an operator product is given by the  $\star$ -product (also known as the Groenewold or Moyal product [30]):*

$$\begin{aligned} W_{\rho\sigma}(u) &= (W_\rho \star W_\sigma)(u) \\ &:= d^{-n} \sum_{v, w} W_\rho(u + v) W_\sigma(u + w) \bar{\chi}([v, w]). \end{aligned}$$

*Proof.* The proofs are all straight-forward; we give only hints on how to conduct them. It will be essential to recall the well-known relation

$$\sum_{x \in \mathbb{Z}_d^n} \chi(xy) = d^n \delta_{y, 0}, \quad (16)$$

for all  $y \in \mathbb{Z}_d^n$ .

Indeed, the first claim can be proven by using Eq. (16) together with the definition of the phase space point operators Eq. (15). Employ Definition 5 and Eq. (16) to establish the second assertion, which in turn implies the third one. Theorem 6.4 makes use of the fact that  $\bar{\chi}(pq) = \prod_i \bar{\chi}(p_i q_i)$ ; see also Section VII for a very similar and more explicit calculation. The validity of the fifth statement is best shown using Eqs. (8), (16).

Let us lastly turn to Claim 6. We have noted that the phase space point operators form an orthonormal system. Hence we can expand an operator  $\rho$  in terms of its Wigner function as  $\rho = \sum_v W_\rho(v) A(v)$ . Substituting  $\rho$  and  $\sigma$  by their respective expansions in  $W_{\rho\sigma}(v) = d^{-n} \operatorname{tr}(A(v) \rho \sigma)$  yields the desired formula with the help of Lemma 29.  $\square$

The following statement will be vital to the proof of the main theorem. It assigns an elegant geometric interpretation to the Clifford group.

**Theorem 7.** (Clifford Covariance) *Let  $U = w(a)\mu(S)$  be a Clifford operation. Let  $\rho' := U\rho U^\dagger$  for some Hermitian operator  $\rho$ . The Wigner function is covariant in the sense that*

$$W_\rho(v) = W_{\rho'}(Sv + a).$$

*Proof.* We compute the action of the Clifford group on the

phase space point operators.

$$\begin{aligned}
& w(a)\mu(S)A(b)\mu(S)^\dagger w(a)^\dagger \\
&= d^{-n} \sum_{v \in V} \bar{\chi}([b, v])w(a)\mu(S)w(v)\mu(S)^\dagger w(a)^\dagger \\
&= d^{-n} \sum_v \bar{\chi}([b, v])w(a)w(Sv)w(a)^\dagger \\
&= d^{-n} \sum_v \bar{\chi}([b, v])\chi([a, Sv])w(Sv) \\
&= d^{-n} \sum_{v':=Sv} \bar{\chi}([b, S^{-1}v'])\bar{\chi}([a, v'])w(v') \\
&= d^{-n} \sum_{v'} \bar{\chi}([Sb + a, v'])w(v') = A(Sb + a).
\end{aligned}$$

The claim follows by use of Eq. (15).  $\square$

Our definition of the discrete Wigner function coincides with the ones used in Refs. [7, 9, 11, 15]. It is further equal to Leonhardt's version [8], up to a permutation of points in phase space; it corresponds to choice (a) in Ref. [12] and lastly to  $G = \mathbb{Z}_d^n$  in Ref. [14]. One can show that  $W$ , as defined here, fulfills the axioms of Ref. [16] which had been laid out in Section IB. Put differently, it is an element of the set of generalized Wigner functions. Gibbons *et al.* remarked in Ref. [16] that among the generalized Wigner functions, some stand out by their high degree of symmetry. In our language, this symmetry is an incarnation of the Clifford covariance established in Theorem 7. Naturally, it is now interesting to ask how much freedom is left in the definition of a Wigner function, once one requires Clifford covariance to hold. We show in Appendix IX B that the definition used here is virtually unique in that regard.

### E. Stabilizer States

Using the composition law of the Heisenberg group Eq. (4), it is easy to see that two Weyl operators  $w(v_1), w(v_2)$  commute if and only if  $[v_1, v_2] = 0$ . Now consider the image of an entire subspace  $M$  under the Weyl representation  $w$ . The set

$$w(M) = \{w(m) | m \in M\}$$

consists of mutually commuting operators if and only if the symplectic form vanishes on  $M$ :

$$[m_1, m_2] = 0, \quad \text{for all } m_i \in M.$$

Spaces of that kind are called *isotropic*. Clearly, if  $M$  is isotropic, then the operators  $w(M)$  can be simultaneously diagonalized. We will see that if  $|M| = d^n$ , the eigenspaces become non-degenerate and can thus be used to single out state vectors in the Hilbert space. A subspace  $M$  of  $V$  is said to be *maximally isotropic* if its cardinality equals  $d^n$ . See Appendix IX C for a justification of that nomenclature.

**Lemma 8.** (Stabilizer States) *Let  $M$  be a maximally isotropic subspace of  $V$ . Let  $v \in V$ . Up to a global phase, there is a unique state vector  $|M, v\rangle$  that fulfills the eigenvalue equations*

$$\chi([v, m])w(m)|M, v\rangle = |M, v\rangle$$

for all  $m \in M$ .

*Proof.* Existence: It is elementary to check that

$$|M|^{-1} \sum_{m \in M} \chi([v, m])w(m) \quad (17)$$

is a rank one projection operator fulfilling the eigenvalue equations.

Uniqueness: According to Appendix IX C, there are  $p^n$  characters of  $M$ , each giving rise to a distinct projection operator as defined in the last paragraph. Two distinct operators of that kind are mutually orthogonal, because they belong to different eigenvalues of at least one of the Weyl operators. But  $\dim \mathcal{H} = |Q| = p^n$  and thus there is no space for more than one-dimensional solutions to the given set of equations.  $\square$

The state vector  $|M, v\rangle$  is called the *stabilizer state* associated to  $M$  and  $v$ . For obvious reasons, one refers to the set of operators  $\{\chi([v, m])w(m) | m \in M\}$  as the *stabilizer* of  $|M, v\rangle$ . Due to the isotropicity of  $M$ , the stabilizer is closed under multiplication and thus constitutes a group. Occasionally, we write  $|M\rangle$  for  $|M, 0\rangle$ . To specify a stabilizer state, we need to specify a maximally isotropic space  $M$ . This is best done by giving a basis  $\{m_1, \dots, m_k\}$  of  $M$ . It is convenient to assemble the basis vectors as the columns of a  $2n \times k$ -matrix, which is generally referred to as the *generator matrix*. As the choice of a basis is non-unique, so is the form of the generator matrix.

A stabilizer state  $|M\rangle$  is a *graph state* if it possesses a generator matrix of the form

$$\begin{pmatrix} \vartheta \\ \mathbb{1}_{n \times n} \end{pmatrix}, \quad (18)$$

where  $\vartheta$  is a symmetric  $n \times n$ -matrix [24]. The designation stems from the fact that  $\vartheta$  can be interpreted as the adjacency matrix of a graph. Many properties of  $|M\rangle$  are describable in terms of that graph alone [24]. Some authors require the diagonal elements  $\vartheta^i_i$  to vanish (equivalently, no vertex of the graph should be linked to itself), but we will not impose that restriction. Note that there exist considerably more general definitions of graph states [19].

Obviously, we will be concerned with Wigner functions of stabilizer states. Lemma 9 clarifies their structure.

**Lemma 9.** (Wigner functions of stabilizer states) *The Wigner function of a stabilizer state  $|M, v\rangle$  is the indicator function on  $M + v$ . More precisely,*

$$W_{|M, v\rangle}(a) = \frac{1}{d^n} \delta_{M+v}(a) = \frac{1}{d^n} \begin{cases} 1 & a \in M + v \\ 0 & \text{else.} \end{cases}$$

*Proof.* The representation given in Eq. (17) of  $|M, v\rangle$  determines the characteristic function

$$\Xi_{|M, v\rangle}(b) = d^{-n} \chi([v, b]) \delta_M(b).$$

We compute the symplectic Fourier transformation:

$$\begin{aligned} (\mathcal{F}_S \Xi_{|M, v\rangle})(a) &= d^{-2n} \sum_{b \in V} \bar{\chi}([a, b]) \chi([v, b]) \delta_M(b) \\ &= d^{-2n} \sum_{b \in M} \bar{\chi}([a - v, b]) \\ &= d^{-n} \delta_{M^\perp}(a - v). \end{aligned}$$

Where

$$M^\perp = \{v \in V \mid [m, v] = 0 \text{ for all } m \in M\}$$

is the *symplectic complement* of  $M$  in  $V$ . But  $M$  is a maximally isotropic space and hence  $M = M^\perp$  (see Appendix IX C).  $\square$

In particular we know now that the Wigner function of stabilizer states is non-negative. The next sections are devoted to the proof of the converse.

### III. DISCRETE HUDSON'S THEOREM

#### A. Bochner's Theorem

Define the *self correlation function*

$$K_\psi(q, x) = \psi(q + 2^{-1}x) \bar{\psi}(q - 2^{-1}x)$$

and note that the Wigner function fulfills

$$W(p, q) = \frac{1}{d^n} \sum_{x \in Q} \bar{\chi}(px) K_\psi(q, x). \quad (19)$$

Fix a  $q_0 \in Q$ . Designating the function  $p \mapsto W(p, q_0)$  by  $W(\cdot, q_0)$ , Eq. (19) says that  $W(\cdot, q_0)$  is the Fourier transform of  $K(q_0, \cdot)$ . Therefore,  $W$  is non-negative if and only if the  $d^n$  functions  $K(q_0, \cdot)$  have non-negative Fourier transforms.

In harmonic analysis, the set of functions with non-negative Fourier transforms is characterized via a theorem due to Bochner. It is usually proven either in the context of Fourier analysis on the real line or else, in full generality, for harmonic analysis on – not necessarily abelian – locally compact groups. While the former statement is not general enough for our purpose, the latter is not easily accessible. However, it turns out that in the discrete abelian setting an elementary proof can be given. It is stated in the next theorem, along with a variation for subsequent use.

**Theorem 10.** (Variations of Bochner's Theorem) *Let  $M$  be a subspace of  $Q$ . Let  $f : M \rightarrow \mathbb{C}$ . It holds that*

1. *The Fourier transform of  $f$  is non-negative if and only if the matrix*

$$A^x_q = f(x - q) \quad (x, q \in M)$$

*is positive semi-definite.*

2. *The Fourier transform of  $f$  has constant modulus (i.e.  $|\hat{f}(x)| = \text{const}$ ) if and only if  $f$  is orthogonal to its translations:*

$$\langle f, \hat{x}(q)f \rangle = \sum_{x \in M} \bar{f}(x) f(x - q) = 0$$

*for all non-zero  $q \in M$ .*

*Proof.* The following computation is a variant of a well-known fact concerning circulant matrices. We claim that any character  $\zeta$  of  $M$  is an eigenvector of  $A$  with eigenvalue  $\lambda = |M|^{-1/2} \hat{f}(\zeta)$ . Indeed, plugging in the definitions yields

$$\begin{aligned} (A\zeta)(x) &= \sum_q A^x_q \zeta(q) \\ &= \sum_q f(x - q) \zeta(q) \\ &= \sum_q f(q) \bar{\zeta}(q) \zeta(x) \\ &= \sqrt{|M|} \hat{f}(\zeta) \zeta(x). \end{aligned}$$

There exist  $|M|$  characters and thus equally many eigenvectors of  $A$ . Therefore,  $A$  can be diagonalized. All its eigenvalues are non-negative if and only if  $\hat{f}$  is non-negative.

By the same argument,  $A$  is proportional to a unitary matrix if and only if  $|\hat{f}(q)|$  is constant. But a matrix is unitary if and only if its rows form an orthonormal set of vectors.  $\square$

From here, the proof proceeds in two steps. Section III B harvests Theorem 10.1 to gain information on the pointwise modulus  $|\psi(q)|$  of a vector with non-negative Wigner function. Building on these findings, we will analyze the properties of such Wigner functions in Section III C.

#### B. Supports and Moduli

**Lemma 11.** (Modulus Inequality) *Let  $\psi$  be a state vector with non-negative Wigner function.*

*It holds that*

$$|\psi(q)|^2 \geq |\psi(q - x)| |\psi(q + x)|$$

*for all  $q, x \in Q$ .*

*Proof.* Fix a  $q \in Q$ . As  $W_\psi$  is non-negative, so is the Fourier transform of  $K_\psi(q, \cdot)$ . Bochner's Theorem implies that the matrix  $A^x_y = K(x - y, q)$  is positive semi-definite which in

turn implies that all principal sub-matrices are psd. In particular the determinant of the  $2 \times 2$  principal sub-matrix

$$\begin{pmatrix} K_\psi(q, 0) & K_\psi(q, 2x) \\ K_\psi(q, -2x) & K_\psi(q, 0) \end{pmatrix} \\ = \begin{pmatrix} |\psi(q)|^2 & \psi(q+x)\bar{\psi}(q-x) \\ \bar{\psi}(q+x)\psi(q-x) & |\psi(q)|^2 \end{pmatrix}$$

must be non-negative. But this means

$$|\psi(q)|^4 - |\bar{\psi}(q+x)\psi(q-x)|^2 \geq 0,$$

which proves the theorem.  $\square$

We will call the set  $\text{supp } \psi$  of points where a state-vector is non-zero its *support*.  $S = \text{supp } \psi$  has the property to contain the *midpoint* of any two of its elements. Indeed, if  $a, b \in S$ , then setting  $q = 2^{-1}(a+b)$  and  $x = 2^{-1}(a-b)$  in the Modulus Inequality shows that

$$|\psi(2^{-1}(a+b))| \geq |\psi(a)| |\psi(b)| > 0,$$

hence  $2^{-1}(a+b) \in S$ . Let us refer to sets possessing this quality as being *balanced*.

The following lemma clarifies the structure of balanced sets. Recall that a subset  $A$  of  $V$  is *affine* if  $A = M + v$  for a subspace  $M$  and some vector  $v$ . An affine space is a subspace if and only if it contains the origin 0.

**Lemma 12.** (Balanced sets) *A subset  $S$  of  $Q$  is balanced if and only if  $S$  is an affine space.*

*Proof.* We show the 'only if' part, the other one being simple.

As both the characterizations of balancedness and affinity are invariant under translation, there is no loss of generality in assuming that  $0 \in S$ . We have to establish that  $S$  is closed under both addition and scalar multiplication.

Let  $a \in S$ . We claim that

$$2^{-l}\lambda a \in S \quad (20)$$

for all  $l \in \mathbb{N}$  and  $\lambda \leq 2^l$ . The proof is by induction on  $l$ . Suppose Eq. (20) holds for some  $l$ . If  $\lambda \leq 2^{l+1}$  is even, then  $2^{-l-1}\lambda a = 2^{-l}(\lambda/2)a \in S$ . Else,

$$2^{-l-1}\lambda a = 2^{-1}\left(2^{-l}\frac{\lambda-1}{2}a + 2^{-l}\frac{\lambda+1}{2}a\right) \in S,$$

which shows the validity of Eq. (20).

There exists an integer  $l > d$  such that  $2^l \equiv 1 \pmod d$ . Indeed, by Euler's Theorem,  $2^{\phi(d)} \equiv 1 \pmod d$ , where  $\phi$  is Euler's totient function. So  $l = d\phi(d)$  satisfies the requirements. Inserting  $l$  into Eq. (20), we conclude that  $\lambda a \in S$  for all  $\lambda \leq 2^d$ . Thus certainly  $\lambda a \in S$  for all  $\lambda \in \mathbb{Z}_d$  and we have proved closure under scalar multiplication.

If  $a, b \in S$  then, by the last paragraph  $2a, 2b \in S$  and hence  $2^{-1}(2a+2b) \in S$ , establishing closure of  $S$  under addition.  $\square$

**Lemma 13.** (Constant Modulus) *Let  $\psi$  be a state vector with non-negative Wigner function. Then  $|\psi(\cdot)|$  is constant on the support of  $\psi$ .*

*Proof.* Pick two points  $x, q \in \text{supp } \psi$  and suppose  $|\psi(q)| > |\psi(x)|$ .

Letting  $z = x - q$ , the assumption reads  $|\psi(q)| > |\psi(q+z)|$ . The Modulus Inequality, centered at  $q + z$ , gives

$$|\psi(q+z)|^2 \geq |\psi(q)| |\psi(q+2z)|. \quad (21)$$

As  $\text{supp } \psi$  is affine, we know that  $\psi(q+kz) \neq 0$  for all  $k \in \mathbb{Z}_d$ . Hence Eq. (21), together with the assumption implies

$$\begin{aligned} |\psi(q+z)|^2 &> |\psi(q+z)| |\psi(q+2z)| \\ \Leftrightarrow |\psi(q+z)| &> |\psi(q+2z)|. \end{aligned}$$

By inducting on this scheme, we arrive at

$$|\psi(q)| > |\psi(q+z)| > |\psi(q+2z)| > \dots$$

and therefore  $|\psi(q)| > |\psi(q+dz)| = |\psi(q)|$ , which is a contradiction.

Thus  $|\psi(q)| \leq |\psi(x)|$ . Swapping the roles of  $x$  and  $q$  proves that equality must hold.  $\square$

At this point, we have full knowledge of the pointwise *modulus* of a state vector with non-negative Wigner function. The *phases* of  $\psi(\cdot)$  are, however, completely unknown. The section to come addresses this problem indirectly, by studying non-negative Wigner functions.

### C. Non-negative Wigner functions

To motivate the following, assume for a moment that  $\psi$  has a non-negative Wigner function and further, that  $\psi(q) \neq 0$  for all  $q$ . Choose a  $q_0 \in Q$  and consider the function  $W(\cdot, q_0)$ . Lemma 13 implies that  $K_\psi(q_0, \cdot)$  has constant modulus and hence – by Theorem 10.2 –  $W(\cdot, q_0)$  must be orthogonal to its translations. Clearly, a non-negative function possesses this property if and only if it is supported on at most a single point.

There hence exists a  $p_0 \in Q$  such that  $W(p, q_0) \propto \delta_{p, p_0}$ . This observation starkly reduces the possible forms of positive Wigner functions; it will be generalized to state vectors with arbitrary support in the next lemma.

**Lemma 14.** *Let  $\psi$  be a state vector. If  $W_\psi$  is non-negative, then it is of the form*

$$W_\psi(v) = d^{-n} \delta_T(v)$$

where  $T \subset V$  is a set of cardinality  $d^n$ .

What is more, if  $0 \in T$ , then the set of elements of  $T$  with vanishing position coordinates

$$\{(p, 0) \in T \mid p \in Q\}$$

is a subspace of  $V$ .

*Proof.* Let  $S = \text{supp } \psi$ . Again, we may assume that  $S$  is a subspace of  $Q$ , for else we replace  $\psi$  by  $w(-s)\psi$  for some  $s \in S$ . It follows that  $\text{supp } K_\psi = S \times S$ . Indeed,

$$\begin{aligned} K_\psi(q, x) \neq 0 &\Leftrightarrow q \pm 2^{-1}x \in S \\ &\Leftrightarrow q \in S \wedge x \in S. \end{aligned}$$



Denote by  $S^\perp = \{q \in Q | sq = 0 \text{ for all } s \in S\}$  the orthogonal complement of  $S$  [44]. We will adopt the common notation  $[p] = p + S^\perp$  for cosets of  $S^\perp$ . It should be clear that  $[p]$  is nothing other but the *affine space* with directional vector space given by  $S^\perp$  and base vector  $p$ . The set  $S^*$  of characters of  $S$  can be identified with  $Q/S^\perp$ . Certainly,  $s \mapsto \chi(ps)$  defines a character of  $S$  for every  $p \in Q$ . Further,  $\chi(ps) = \chi(p's)$  for all  $s \in S$  if and only if  $p - p' \in S^\perp$ . That indeed all elements of  $S^*$  can be obtained this way is shown in Corollary 26.

Define  $K'_\psi$  to be the restriction of  $K_\psi$  to its support  $S \times S$ . For the rest of the proof, we fix a  $q_0 \in S$ . Now consider

$$\begin{aligned} W(p, q_0) &= d^{-n} \sum_{x \in Q} \bar{\chi}(px) K(q_0, x) \\ &= d^{-n} \sum_{x \in S} \bar{\chi}(px) K'(q_0, x). \end{aligned}$$

Viewed as a function in  $p$ ,  $W(p, q_0)$  has constant values on cosets of  $S^\perp$ . Therefore,

$$W'([p], q) := d^n |S|^{-1/2} W(p, q) \quad (22)$$

is a well-defined function on  $S^*$ . The considerations of the previous paragraph allow us to identify  $W'([ \cdot ], q_0)$  as the Fourier transform of  $K'(q_0, \cdot)$ .

We can now repeat the argumentation presented just before the current lemma. Indeed, the modulus of  $K'(q_0, [ \cdot ])$  is constant and  $W'$  is non-negative. Furthermore, by definition of  $q_0$ ,  $K'(q_0, [ \cdot ])$  is non-zero and we may thus conclude that  $p \mapsto W'([p], q_0)$  is supported on exactly one coset  $[p_0]$ .

Normalization of  $\psi$  implies  $|\psi(\cdot)| = |S|^{-1/2}$ . Hence  $|K'_\psi(q_0, \cdot)| = |S|^{-1}$  and

$$\|K'_\psi(q_0, \cdot)\|^2 = \sum_x |K'_\psi(q_0, x)|^2 = |S|^{-1}.$$

By Parseval's Theorem,  $\|W'([ \cdot ], q_0)\|^2 = |S|^{-1}$  as well. It follows that  $W'([p_0], q_0) = |S|^{-1/2}$ .

Inverting Eq. (22) gives

$$W(p, q) = d^{-n} \begin{cases} 1 & [p] = [p_0] \\ 0 & \text{else} \end{cases} \quad (23)$$

which proves the first claim of the lemma. The cardinality of  $T$  is fixed by the normalization of the Wigner function (Theorem 6.6).

Now suppose  $W(0, 0) = W'([0], 0) \neq 0$ . Clearly, then  $W(p, 0)$  is non-zero if and only if  $p \in [0] \Leftrightarrow p \in S^\perp$ . The last assertion of the lemma follows, since  $S^\perp$  is a subspace of  $Q$ .  $\square$

So a non-negative Wigner function is the indicator functions of some set  $T$ . This finding is compatible with Lemma 9, which describes the structure of Wigner functions of stabilizer states. The next two lemmas verify that  $T$  has indeed all the properties of the sets that appear in Lemma 9.

**Lemma 15.** *Let  $\psi$  be a state vector. If  $W_\psi$  is of the form*

$$W_\psi(v) = d^{-n} \delta_T(v),$$

*then  $T$  is an affine space.*

*Proof.* The proof proceeds similar to the one of Lemma 12. There is no loss of generality in assuming that  $0 \in T$ .

First, we show that  $T$  is closed under scalar multiplication. To this end, pick a point  $a \in T$ . There exists a symplectic mapping  $S$  that sends  $a$  to a vector  $a'$  of the form  $(a'_p, 0)$  where  $a'_p \in Q$  (see Appendix IX D). The set  $T' = ST$  is the support of the Wigner function of  $\mu(S)\psi$ . By the second assertion of Lemma 14,  $\lambda a' \in ST$  for every  $\lambda \in \mathbb{Z}_d$ . Hence  $S^{-1}(\lambda a') = \lambda a \in T$ .

Turning to closedness under addition, let  $a, b \in T$ . By the last paragraph,  $2a, 2b \in T$ . Arguing as before, note that the set  $T - 2a$  is the support of the Wigner function of  $w(-2a)\psi$  and thus closed under multiplication. As  $2b - 2a \in T - 2a$ , we know that  $b - a \in T - 2a$  and hence  $b + a \in T$ .  $\square$

**Lemma 16.** *Let  $\psi$  be a state vector such that  $W_\psi$  is of the form*

$$W_\psi(v) = d^{-n} \delta_T(v).$$

*If  $T$  is a subspace, then it is isotropic.*

*Proof.* The vector  $\psi$  describes a pure state, hence  $W_\psi \star W_\psi = W_\psi$  (recall the Moyal product, introduced in Theorem 6). Let  $u \in T$ . Plugging in the definitions gives

$$\begin{aligned} W_\psi \star W_\psi(u) &= d^{-n} \sum_{v, w \in V} W_\psi(u + v) W_\psi(u + w) \bar{\chi}([v, w]) \\ &= d^{-3n} \sum_{v, w \in T} \bar{\chi}([v, w]). \end{aligned}$$

Note that  $\sum_{w \in T} \bar{\chi}([v, w]) \leq |T| = d^n$  with equality if and only if  $[v, w] = 0$  for all  $w$ . Hence

$$W_\psi \star W_\psi(u) \leq d^{-n} = W_\psi(u).$$

For the left-hand and the right-hand side to be equal,  $T$  must be isotropic.  $\square$

Therefore  $T$ , as defined above, is of the form  $T = M + v$  where  $M$  is an isotropic space of cardinality  $d^n$ . But then,  $W_\psi$  is the Wigner function of a stabilizer state, by Lemma 9. We have proven:

**Theorem 17.** (Main Theorem) *Let  $\psi \in L^2(\mathbb{Z}_d^n)$  be a state vector. If the Wigner function of  $\psi$  is non-negative, then  $\psi$  is a stabilizer state.*

#### IV. DISCRETE GAUSSIANS

It has long been realized that the coefficients of stabilizer state vectors are described by quadratic forms. However, the current literature either neglects the non-prime case (Refs. [19, 20, 26]) or is less explicit (Ref. [21]) than the following lemma in showing the tight relation between Gaussian states and stabilizer states.

We will concentrate on stabilizer states with full support. This constitutes only a modest restriction of generality. Indeed, let  $\psi$  be a general stabilizer state, let  $Q' := \text{supp } \psi$ . Let us for the sake of simplicity assume that  $d$  is prime and  $Q'$  is a subspace of  $Q$ . The restriction of the coordinate function  $\psi(q)$  to  $Q'$  can be thought of as defining a vector  $\psi'$  of a quantum state of an  $n' := \dim Q'$  particle system. It is now possible to check that  $\psi'$  is a stabilizer state. In this way any stabilizer state can be viewed as one with full support, possibly on a smaller system. We will, however, not take the time to make this construction precise nor will we rely on it in this paper.

**Lemma 18.** *Let  $\psi$  be a state vector. The following statements are equivalent.*

1.  $\psi$  is a stabilizer state and  $\psi(q) \neq 0$  for all  $q \in Q$ .
2. Up to the action of a Weyl operator,  $\psi$  is a graph state.
3. There exists a symmetric  $n \times n$ -matrix  $\theta$  and an  $x \in Q$  such that

$$\psi(q) = \omega^{q\theta q + xq}.$$

*Proof.* (1  $\Rightarrow$  2). By assumption  $|\psi\rangle = |M, v\rangle$  for some maximal isotropic space  $M$  and a vector  $v$ . We claim that there is no non-zero  $p \in Q$  such that  $(p, 0) \in M$ .

For suppose there exists such a  $p$ . Then

$$\langle q | w(p, 0) | M \rangle = \chi(-pq) \langle q | M \rangle.$$

On the other hand,

$$\langle q | w(p, 0) | M \rangle = \bar{\chi}([v, (p, 0)]) \langle q | M \rangle,$$

by the definition of  $|M, v\rangle$ . Hence  $\text{supp } |M\rangle$  must be contained within a hyper-surface of  $Q$  specified by  $pq = \text{const}$ , which contradicts the assumption that  $\text{supp } \psi = Q$ .

There are  $d^n$  elements in  $M$ . By the last paragraph, no two of them have the same position coordinates. As there exist only  $d^n = |Q|$  possible choices for the position coordinates, one can find for every  $q \in Q$  a  $p \in Q$  such that  $(p, q) \in M$ . Let  $e_1, \dots, e_n$  denote the canonical basis of  $\mathbb{Z}_d^n$ . Choose  $m_1, \dots, m_n \in M$  such that the position part of  $m_i$  equals  $e_i$ . The span of  $\{m_i\}_{i=1, \dots, n}$  has clearly cardinality  $d^n$ , so we have found a basis of  $M$ . By construction, the generator matrix composed of these basis vectors has the form shown in Eq. (18) with some  $n \times n$ -matrix  $\theta$ . It is not hard to see that  $M$  is isotropic if and only if  $\theta$  is symmetric, establishing that  $|M\rangle$  is a graph state. Theorem 7 and Lemma 9 show that  $w(v)|M\rangle = |M, v\rangle = |\psi\rangle$ .

(2  $\Rightarrow$  3). Let  $M$  be an isotropic space which possesses a generator matrix of the form given in Eq. (18). Let  $m_i = (\vartheta_i, e_i)$  be the  $i$ th column of that matrix. We need to establish the existence of a symmetric matrix  $\theta$  and an  $x \in Q$  such that

$$\langle q | M, v \rangle = \omega^{q\theta q + xq} =: \psi(q).$$

Indeed, choose

$$\theta = 2^{-1}\vartheta, \quad x_i = [v, m_i].$$

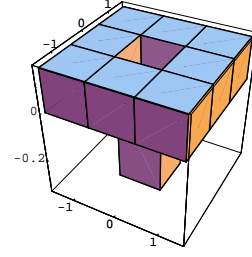


FIG. 1: Wigner function of the antisymmetric vector  $|\psi_{-}\rangle$ .

Using Eq. (8), one can then check by direct computation that  $\psi$  fulfills the defining eigenvalue equations

$$\chi([v, m_i])w(m_i)\psi = \psi$$

and hence  $|\psi\rangle = |M, v\rangle$ , by Lemma 8.

(3  $\Rightarrow$  1). Reverting the previous proof shows that  $\psi$  is a graph state. It has maximal support by definition.  $\square$

The claimed analogy between stabilizer states and Gaussian states is apparent when comparing statement 3 to Theorem 1.

## V. MIXED STATES

It is natural to ask how the results obtained before generalize to mixed states. Certainly, mixtures of stabilizer states are non-negative on phase space and it might be surmised that all such quantum states are convex combinations of stabilizer ones. In the context of continuous variable systems, Bröcker and Werner refuted an analogous conjecture by giving a counter-example [31]. Again, the situation is similar in the finite setting, as will be shown now.

As a consequence of Theorem 6.5,  $A(0)$  can be decomposed as  $A(0) = P_{+} + P_{-}$ , where  $P_{\pm}$  denotes the projector onto the symmetric and antisymmetric state vectors respectively. Since  $P_{+} + P_{-} = \mathbb{1}$ , we have that  $P_{-} = 1/2(\mathbb{1} - A(0))$ . Because we know the Wigner functions of both  $\mathbb{1}$  ( $W(v) = d^{-n}$ ) and of  $A(0)$  ( $W(v) = \delta_{v,0}$ ), we immediately obtain

$$W_{P_{-}}(v) = \frac{1}{2} \begin{cases} d^{-n} - 1 & v = 0 \\ d^{-n} & \text{else.} \end{cases} \quad (24)$$

For a single three-dimensional quantum system there exists a unique antisymmetric state vector  $|\psi_{-}\rangle = 2^{-1/2}(|+1\rangle - |-1\rangle)$ , hence  $P_{-} = |\psi_{-}\rangle\langle\psi_{-}|$ . Figure 2 depicts the Wigner function of the state  $\rho$ , obtained by mixing the pure states  $|\psi_{-}\rangle, w(-1, 0)|\psi_{-}\rangle, w(-1, -1)|\psi_{-}\rangle$  with equal weights.

The Wigner function of a single-particle stabilizer state is a line in the two-dimensional phase space, according to Lemma 9. There are  $d(d+1)$  such lines and hence equally many stabilizer states. Assume these states have been brought into some order and denote the associated projection operators by  $P_1, \dots, P_{d(d+1)}$ . Let  $\rho = \sum_i^{d(d+1)} \lambda_i P_i$  be a convex decomposition of  $\rho$  in terms these operators. If there is a point  $v$  in phase space where  $W_{\rho}(v) = 0$  and  $W_{P_i}(v) \neq 0$ , then clearly

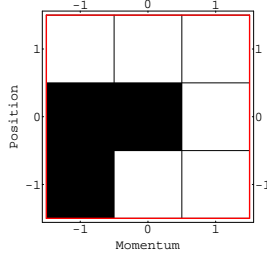


FIG. 2: Wigner function of the equal mixture of the vectors  $|\psi_-\rangle$ ,  $w(-1, 0)|\psi_-\rangle$  and  $w(-1, -1)|\psi_-\rangle$ . White squares stand for a value of  $1/6$ , black squares for 0.

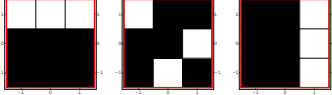


FIG. 3: The white squares mark all lines in  $\mathbb{Z}_3^2$  that do not intersect any point where the Wigner function shown in Fig. 2 vanishes.

$\lambda_i$  must vanish. By exhaustively listing all 12 lines in  $\mathbb{Z}_3^2$ , one finds that  $\rho$  can have non-zero coefficients only with respect to the stabilizer states whose Wigner functions are shown in Figure 3.

But  $\rho$  admits no convex decomposition in terms of these three lines. Indeed, no two of them cover all the points in the support of  $W_\rho$ , so only a mixture of all three lines could potentially suffice. Now notice that the point  $(1, -1)$  is an element only of the third line, while  $(1, 0)$  is contained in both the second and the third one. Therefore any mixture of these three lines takes on a higher value on  $(1, 0)$  than on  $(1, -1)$ . The distribution  $W_\rho$ , on the other hand, is constant on its support.

## VI. DYNAMICS

Having established which quantum states give rise to non-negative phase space distributions, the next step is to characterize the set of operations that preserve this property. We have seen in Section IID that Clifford unitaries implement permutations in phase space and thus manifestly preserve positivity. They are unique in that regard, as will be shown now.

By the results of Section III, it is apparent that a unitary operation  $U$  can preserve positivity only if it sends stabilizer states to stabilizer states. One can reasonably conjecture that only Clifford operations possess this feature and in the case of single-particles in prime-power dimensions, a proof of this fact has been given in Ref. [27]. The general case, however, poses surprising difficulties which have forced us to take a less direct route.

Let us shortly pause to clarify our objectives. We aim to characterize the set of unitaries  $U$  that satisfy statements of the kind:  $W_{U\rho U^\dagger}$  is non-negative whenever  $W_\rho$  is. We can require the above statement to hold for *any* Hermitian operator  $\rho$ , or just whenever  $\rho$  is a *quantum state*. In the former case the restrictions on  $U$  are much stronger than in the latter one.

Indeed, by considering the image of the phase space point operators  $A(a)$  under the action of  $U$  and making use of Lemma 29, it is straight-forward to prove that only Clifford operations can preserve positivity of the Wigner functions of general Hermitian operators. The following theorem is slightly more ambitious in considering only the action of  $U$  on quantum states.

**Theorem 19.** (Only permutations preserve positivity). *Let  $U$  be unitary. If, for all quantum states  $\rho$  with non-negative Wigner function, it holds that  $W_{U\rho U^\dagger}$  is non-negative, then  $U$  is Clifford.*

*Proof.* Firstly, take a note that substituting ‘quantum state’ by ‘positive operator’ in the above theorem, only amounts to a change of normalization and does not alter the statement. Set

$$\mu(\rho) := \min_{v \in V} W_\rho(v),$$

$$\nu(\rho) := \text{minarg } W_\rho := \{v \in V | W_\rho(v) = \mu(\rho)\}.$$

Let  $\rho$  be such that  $\mu(\rho) < 0$ . We claim that  $\mu(\rho) = \mu(\rho')$ , where  $\rho' = U\rho U^\dagger$ . In other words:  $U$  preserves minimal values.

Indeed, there exists positive constants  $\lambda_{1,2}$  such that

$$\lambda_1 \mu(\rho') + \lambda_2 d^{-n} = 0.$$

Hence  $\sigma := \lambda_1 \rho + \lambda_2 \mathbb{1}$  has a non-negative Wigner function. The assumption  $\mu(\rho') < \mu(\rho)$  yields

$$W_{U\sigma U^\dagger}(v) = \lambda_1 \mu(\rho') + \lambda_2 d^{-n} < 0$$

for every  $v \in \nu(\rho')$ , which contradicts the defining property of  $U$ . Thus  $\mu(\rho') \leq \mu(\rho)$ . Substituting  $U$  by  $U^{-1}$  shows that equality of  $\mu(\rho)$  and  $\mu(\rho')$  must hold.

Now set

$$\rho(a) := (1 - d^{-n})^{-1} w(a) P_- w(a)^\dagger$$

for all  $a \in V$ . We have  $\mu(\rho(a)) = \mu(\rho'(a)) = -1$  and  $\nu(\rho) = \{a\}$ . The crucial observation lies in the fact that  $\nu(\rho')$  contains only a single point as well. So,  $U$  preserves the ‘pointed’ shape of  $W_\rho(a)$ . To see why that is the case, suppose there is a  $a_0$  such that  $|\nu(\rho(a_0)')| > 1$ . There are  $d^{2n}$  operators  $\rho(a)'$  and equally many points in phase space, so there exists an  $a_1$  such that  $\nu(a_0)$  and  $\nu(a_1)$  intersect in at least one point  $v$ . Define  $\sigma = 1/2(\rho(a_0) + \rho(a_1))$ . It holds that  $\mu(\sigma) > -1/2$ , whereas  $W_{\sigma'}(v) = -1$  which is a contradiction. There is hence a well-defined function  $S$  which sends  $a$  to the unique element of  $\nu(\rho(a)')$ .

Finally, let  $\sigma$  be any density matrix. The idea is to mix  $\sigma$  very weakly to  $\rho(a)$ , so that the positions of the minima of the mixture are still determined by  $\rho(a)$ . Indeed, there exists an  $\epsilon > 0$  such that

$$\nu(\rho(a) + \epsilon\sigma) = \{a\}$$

$$\mu(\rho(a) + \epsilon\sigma) = -1 + \epsilon W_\sigma(a);$$

$$\nu(\rho(a)' + \epsilon\sigma') = \{S(a)\}$$

$$\mu(\rho(a)' + \epsilon\sigma') = -1 + \epsilon W_\sigma(S(a)).$$

Hence  $W_{\sigma'}(Sa) = W_\sigma(a)$ . We have established that  $U$  acts as a permutation in phase space and is therefore Clifford by Lemma 29.  $\square$

## VII. PRIME POWER DIMENSIONS

Wigner functions for quantum systems with prime power dimensions have received particular attention in the literature (most prominently in Ref. [16]). Once again, this is due to the fact that a finite field of order  $d$  exists exactly when  $d$  is the power of a prime and that the field's well-behaved geometrical properties facilitate many constructions. The present section briefly addresses the relationship between three natural approaches to Wigner functions for such systems. We assume the reader is already familiar with the definition of Weyl operators over Galois fields; a thorough introduction can be found in Refs. [15, 16].

Let  $d = p^k$  for some prime number  $p$ . There are three natural ways of associating a configuration space to  $\mathcal{H}$ . These are

1. an  $n$ -dimensional vector space over  $\mathbb{Z}_p$ ,
2. a one-dimensional module over  $\mathbb{Z}_{p^n}$  or
3. a one-dimensional vector space over the Galois field  $\mathbb{F}_{p^n}$  of order  $p^n$ .

The first and the second of these points of view have manifestly been covered in this paper. So far we neglected case 3, because – as we will see – it can be completely reduced to the first one.

Let us quickly gather some well-known facts on finite fields. If  $p$  is prime and  $n$  a positive integer,  $\mathbb{F}_{p^n}$  denotes the unique finite field of order  $d = p^n$ . The simplest case occurs for  $n = 1$ , when  $\mathbb{F}_p \simeq \mathbb{Z}_p$ . For  $n > 1$ , fields  $\mathbb{F}_{p^n}$  are realized by *extending*  $\mathbb{F}_p$ , which is then referred to as the *base field*. Extension fields contain the base field as a subset. The extension field possesses the structure of an  $n$ -dimensional vector space over the base field. A set of elements of  $\mathbb{F}_{p^n}$  is a *basis* if it spans the entire field under addition and  $\mathbb{F}_p$ -multiplication. After having chosen a basis  $\{b_1, \dots, b_n\}$ , we can specify any element  $f = \sum_i f^i b_i$  by its expansion coefficients  $\{f^i\}$ . The operation

$$\text{Tr } f = \sum_{k=0}^{n-1} f^{p^k}$$

takes on values in the base field and is  $\mathbb{F}_p$ -linear. Therefore,

$$\langle f, g \rangle \mapsto \text{Tr}(fg)$$

defines an  $\mathbb{F}_p$ -bilinear form. For any basis  $\{b_i\}$ , there exists a *dual basis*  $\{b^i\}$  fulfilling the relation  $\text{Tr}(b^i b_j) = \delta_{i,j}$  (we do not use Einstein's summation convention). From now on, we assume that a basis  $b_i$  and a dual one  $b^i$  have been fixed.

Repeating the construction put forward in Section II, we introduce the Hilbert space  $\mathcal{H} = L^2(\mathbb{F}_{p^n})$ , in other words,  $\mathcal{H}$  is the span of  $\{|q\rangle | q \in \mathbb{F}_{p^n}\}$ . The choice of a basis induces a tensor structure on  $\mathcal{H}$  via

$$|q\rangle = \left| \sum_i q^i b_i \right\rangle \mapsto \bigotimes_i |q^i\rangle.$$

We obtain a character of  $\mathbb{F}_{p^n}$  by setting  $\chi_{p^n}(f) = \chi_p(\text{Tr } f)$ . Note that for  $n = 1$ ,  $\chi_{p^n} = \chi_p$ . Expanding momentum coordinates  $p = \sum_j p_j b^j$ , the character factors:

$$\chi(pq) = \chi_p\left(\sum_{i,j} p_j q^i \text{Tr}(b_i b^j)\right) = \prod_i \chi_p(p_i q^i).$$

Similarly, the shift and multiply operators factor with respect to this tensor structure:

$$\begin{aligned} x\left(\sum_i q^i b_i\right) \left| \sum_j x^j b_j \right\rangle &= \bigotimes_i x^{(i)}(q^i) |x^i\rangle \\ z\left(\sum_i p_i b^i\right) \left| \sum_j x^j b_j \right\rangle &= \prod_i \chi_p(p_i x^i) \left| \sum_j x^j b_j \right\rangle \\ &= \bigotimes_i z^{(i)}(p_i) |x^i\rangle, \end{aligned}$$

where  $x^{(i)}$  and  $z^{(i)}$  act on the  $i$ th  $p$ -dimensional subsystem. A straight-forward computation along the lines just presented shows that both the Weyl operators and the phase space point operators factor:

$$\begin{aligned} w(p, q) &= \bigotimes_i w^{(i)}(p_i, q^i) = w(p_1, \dots, p_n, q^1, \dots, q^n) \\ A(p, q) &= \bigotimes_i A^{(i)}(p_i, q^i) = A(p_1, \dots, p_n, q^1, \dots, q^n). \end{aligned}$$

The above result thus states that the Wigner function induced by the choice  $Q = \mathbb{F}_{p^n}$  coincides – up to re-labeling of the phase space points – with the one for  $Q = \mathbb{F}_p^n$ . In particular, both definitions give rise to the same set of states with a non-negative phase space distribution.

For stabilizer states, however, the situation is not as easy, as will be discussed subsequently. The preceding discussion suggests defining a map  $\iota : \mathbb{F}_{p^n}^{2n} \rightarrow \mathbb{F}_p^{2n}$  by

$$(p, q) \mapsto (p_1, \dots, p_n, q^1, \dots, q^n)$$

(see Refs. [15, 32]). Let  $M$  be a maximal isotropic subspace of  $\mathbb{F}_{p^n}^{2n}$ . It is readily verified that  $\iota(M) \subset \mathbb{F}_p^{2n}$  is again isotropic and a subspace. Further, we have shown that the sets of Weyl operators  $w(M)$  and  $w(\iota(M))$  coincide and hence so do the stabilizer states  $|M\rangle$  and  $|\iota(M)\rangle$ .

The converse is not true.  $\iota^{-1}$  does not necessarily map  $\mathbb{F}_p^{2n}$  subspaces to those of  $\mathbb{F}_{p^n}^{2n}$ . More precisely, if  $M \subset \mathbb{F}_p^{2n}$  is a subspace, then  $\iota^{-1}(M)$  can easily be proven to be closed under addition, but will in general fail to be closed under  $\mathbb{F}_{p^n}$ -scalar multiplication. This proves the remark made in the introduction, namely that the set of 'single-particle' (i.e.  $\mathbb{F}_p^{2n}$ ) stabilizer states is a true subset of corresponding 'multi-particle' set. The following subsection gives a quantitative account of the relation of the sets.

### A. Counting stabilizer codes

We are going to count the number of stabilizer states of a system composed of  $n$   $d$ -level particles. In fact, the computation given below is slightly more general in that it gives the number of  $k$ -dimensional *stabilizer codes* [17].

Stabilizer codes are generalizations of stabilizer states. Recall Eq. (17), where we showed that summing Weyl operators  $w(m)$  over the elements  $m$  of a maximal isotropic subspace  $M$  of  $V$  yields a one-dimensional projection operator. It can be shown that if the requirement of maximality is dropped, the sum still evaluates to a projector. The range of this operator is the *stabilizer code* defined by  $M$ . The dimension  $m$  of  $M$  and the dimension  $k$  of the stabilizer code are related by  $k = d^{n-m}$ .

**Theorem 20.** (Number of isotropic subspaces) *Let  $V$  be a  $2n$ -dimensional symplectic vector space over  $\mathbb{F}_d$ , where  $d$  is the power of a prime. The number of  $m$ -dimensional isotropic subspaces of  $V$  is given by*

$$\text{Iso}(n, m, d) = \begin{bmatrix} n \\ m \end{bmatrix}_d \prod_{i=0}^{m-1} (d^{n-i} + 1),$$

where the square brackets denote the Gaussian coefficients

$$\begin{bmatrix} n \\ m \end{bmatrix}_d = \prod_{i=0}^{m-1} \frac{d^{n-i} - 1}{d^{m-i} - 1}.$$

*Proof.* The proof is inspired by a method employed in Ref. [33] to solve a related problem. We count the number of linearly independent  $m$ -tuples consisting of mutual orthogonal vectors. Indeed, as the first vector  $v_1$  we are free to choose any non-zero element of  $V$ . There are  $d^{2n} - 1$  such choices. The second vector must lie in the symplectic complement of the span of the first vector  $\langle v_1 \rangle^\perp$ . Hence,  $v_2$  can be chosen from a  $2n - 1$ -dimensional vector space, the only restriction being that  $v_2 \notin \langle v_1 \rangle$ . It follows that there exist  $d^{2n-1} - d^1$  possibilities for  $v_2$ . Inducting on this scheme gives

$$\prod_{i=0}^{m-1} (d^{2n-i} - d^i) \quad (25)$$

such tuples.

However, since two different tuples might correspond to the same isotropic space, Eq. (25) over-counted the subspaces. To take that fact into account, we must divide by the number of bases within an  $m$ -dimensional space. Arguing in a similar fashion as before, we arrive at  $\prod_{i=0}^{m-1} (d^m - d^i)$  for the sought-for number (see also Ref. [33]). Division gives

$$\text{Iso}(n, m, d) = \prod_{i=0}^{m-1} \frac{d^{2n-i} - d^i}{d^m - d^i} = \prod_{i=0}^{m-1} \frac{d^{2(n-i)} - 1}{d^{m-i} - 1}.$$

Expanding  $d^{2(n-i)} - 1 = (d^{n-i} - 1)(d^{n-i} + 1)$  and using the definition of the Gaussian coefficients concludes the proof.  $\square$

**Corollary 21.** *The number of  $d^{n-m}$ -dimensional stabilizer codes defined on  $n$   $d$ -level systems is*

$$\text{Stabs}(n, m, d) = d^m \begin{bmatrix} n \\ m \end{bmatrix}_d \prod_{i=0}^{m-1} (d^{n-i} + 1).$$

In particular, the number of stabilizer states is

$$\text{Stabs}(n, n, d) = d^n \prod_{i=1}^n (d^i + 1).$$

*Proof.* We only need to justify the pre-factor  $d^m$ . The defining Eq. (17) generates a projector onto a stabilizer code given an isotropic space  $M$  and a character  $\chi([v, \cdot])$  on  $M$ . If  $\dim M = m$ , then there are  $|M| = d^m$  distinct such characters (see Appendix IX C).  $\square$

We can now compare the number of stabilizer states for  $n$  particles of dimension  $d$  to the corresponding number for a single  $d^n$ -dimensional system:

$$\begin{aligned} \frac{\text{Stabs}(n, n, d)}{\text{Stabs}(1, 1, d^n)} &= \frac{\prod_{i=1}^n (d^i + 1)}{d^n + 1} = \prod_{i=1}^{n-1} (d^i + 1) \\ &\geq d^{\sum_{i=1}^{n-1} i} = d^{\frac{1}{2}(n^2 - n)}. \end{aligned}$$

This is the super-exponential scaling mentioned in the introduction.

## VIII. ACKNOWLEDGMENTS

The author is grateful for support and advice provided by Jens Eisert during all stages of this project.

Thanks to Dirk Schlingemann for enlightening conversations on phase space techniques. The figures were produced using *Mathematica* notebooks [15] partly based on Timo Felbinger's `qmatrix` package [39]. Martin Plenio and Alessio Serafini gave helpful comments on draft versions of this paper. Useful references were pointed out to the author by S. Chaturvedi, C. K. Zachos, A. Klimov, and M. Ruzzi.

This work has benefitted from funding provided by the European Research Councils (EURYI grant of J. Eisert), the European Commission (Integrated Project QAP), the EPSRC (Interdisciplinary Research Collaboration IRC-QIP), and the DFG.

## IX. APPENDIX

### A. Discrete Stone-von Neumann Theorem

This section generalizes well-known results for prime-power dimensions (see e.g. Ref. [34] and citations therein) to all odd  $d$ . The proof is based on some simple observations employing group representation theory. We state a preparing lemma beforehand.

**Lemma 22.** *The Weyl representation is irreducible.*

*Proof.* We compute

$$\begin{aligned} \frac{1}{|H(\mathbb{Z}_d^n)|} \sum_{\substack{a \in V, \\ t \in \mathbb{Z}_d}} |\text{tr } w(a, t)|^2 &= d^{-(2n+1)} \sum_t |\text{tr } w(0, t)|^2 \\ &= d^{-(2n+1)} \sum_t d^{2n} = 1 \end{aligned}$$

which establishes irreducibility by a well-known criterion from group representation theory (see any textbook on that topic, e.g. [35]).  $\square$

*Proof. (of Theorem 3)* By the composition law Eq. (4) it is clear that  $w'(p, q, t) := w(S(p, q), t)$  is a representation of the Heisenberg group which affords the same character (i.e.  $\text{tr } w(a, t) = \text{tr } w'(a, t)$ ). The preceding lemma yields that  $w$  and  $w'$  are equivalent and thus the existence of  $\mu(S)$  follows. Further,

$$\begin{aligned} \mu(S)\mu(T)w(p, q)\mu(T)^\dagger\mu(S)^\dagger &= \mu(S)w(T(p, q))\mu(S)^\dagger \\ &= w(ST(p, q)) \\ &= \mu(ST)w(p, q)\mu(ST)^\dagger. \end{aligned}$$

Because the Weyl matrices span the set of all operators, the last line fixes  $\mu(ST)$  modulo a phase and we have proven the second assertion.

We turn to the last claim. Let  $S$  and  $c$  be as defined in Eq. (10). Using the commutation relations Eq. (4) and the fact that conjugation by unitaries leaves the center  $\chi(t)\mathbb{1}$  of the Weyl representation invariant, it is easy to see that  $S$  must be an isometry in the sense that  $[Sa, Sb] = [a, b]$ . To proceed, consider the following calculation. On the one hand

$$\begin{aligned} Uw(a)w(b)U^\dagger &= Uw(a+b, 2^{-1}[a, b])U^\dagger \\ &= w(S(a+b), 2^{-1}[a, b])c(a+b), \end{aligned} \quad (26)$$

while on the other hand,

$$\begin{aligned} Uw(a)w(b)U^\dagger &= Uw(a)U^\dagger Uw(b) \\ &= w(Sa)w(Sb)c(a)c(b) \\ &= w(Sa+Sb, 2^{-1}[Sa, Sb])c(a)c(b). \end{aligned} \quad (27)$$

Comparing the last lines of Eqs. (26) and (27) one finds that  $S$  must be compatible with addition in  $\mathbb{Z}_d^{2n}$  meaning that  $S(a+b) = Sa+Sb$ . Because  $\mathbb{Z}_d$  is cyclic the preceding property implies that  $S$  is also compatible with scalar multiplication:

$$S(\lambda a) = S(a + \dots + a) = S(a) + \dots + S(a) = \lambda S(a).$$

Hence  $S$  is linear and therefore symplectic. Lastly, again using lines (26) and (27), we have that  $c(a+b) = c(a)c(b)$  and conclude that  $c$  is a character. By Lemma 24, there exists an  $a_0 \in V$  such that  $c(\cdot) = \chi([a_0, S \cdot])$ . Thus:

$$\begin{aligned} w(a_0)\mu(S)w(a)\mu(S)^\dagger w(a_0)^\dagger &= w(a_0)w(Sa)w(-a_0) \\ &= \chi([a_0, Sa])w(Sa) \\ &= c(a)w(Sa). \end{aligned}$$

$\square$

## B. Axiomatic Characterization of the Wigner function

The discussion in Section IID should suggest that Definition 5 yields 'the' natural analogue of the original continuous Wigner function. However, to bolster that claim with more objective arguments, we establish that – at least in prime dimensions – the form is virtually determined by the property of Clifford covariance (Theorem 7).

**Theorem 23.** (Uniqueness) *Let  $d$  be an odd prime. Let  $Q, V, \mathcal{H}$  be as usual. Consider a mapping  $W'$  that fulfills the following axioms.*

1. (Phase space)  $W'$  is a linear mapping sending operators to functions on the phase space  $V$ .
2. (Clifford covariance)  $W'$  is covariant under the action of the Clifford group, in the sense of Theorem 7.

*Then  $W'_\rho(p, q) = \lambda_1 W_\rho(p, q) + \lambda_2$  for two constants  $\lambda_{1,2}$ . If further,*

3. (Marginal probabilities)  $W'$  gives the correct marginal probabilities, as stated in Theorem 6.3,

*then  $W'(p, q) = W(p, q)$ .*

*Proof.* Consider an alternative definition  $\rho \mapsto W'_\rho$  of a Wigner function. Linearity implies the existence of a set of operators  $\{A'(v)\}$  such that  $W'(v) = d^{-n} \text{tr}(A'(v)\rho)$ .  $W'$  is covariant under the action of the Weyl operators if and only if  $A'(v) = w(v)A'(0)w(v)^\dagger$ . So the only degree of freedom left in the definition of  $W'$  is the choice of  $A'(0)$ . Again, one must require  $A'(Sv) = \mu(S)A(v)\mu(S)$  if Theorem 7 is to hold. In particular, because the origin 0 is a fixed point of any linear operation,  $A'(0)$  must commute with all  $\mu(S)$ .

As a consequence, the old, unprimed Wigner function  $W_{A'(0)}$  of  $A'(0)$  stays fixed under any symplectic operation  $S$ . Since any two non-zero points of  $V$  can be mapped onto each other by a suitable symplectic matrix  $S$ ,  $W_{A'(v)}$  must be constant on all such points. So there are only two parameters free to be chosen:  $W_{A'(0)}(0)$  and  $W_{A'(0)}(v)$ ,  $v \neq 0$ . Clearly, the set of all operators that comply with these constraints is spanned by  $\mathbb{1}$  and  $A(0)$ :

$$A'(0) = \lambda_1 \mathbb{1} + \lambda_2 A(0). \quad (28)$$

The above decomposition implies the first statement of the Theorem.

As for the second claim, choose an  $a \in V$ . The projection operator  $|a\rangle\langle a|$  is invariant under the action of Weyl operators of the form  $w(p, 0)$ . Thus, due to Clifford covariance, the Wigner function  $W'_{|a\rangle}$  must be  $p$ -shift invariant:  $W'_{|a\rangle}(p+p', q) = W'_{|a\rangle}(p, q)$ . We required Theorem 6.3 to hold, hence

$$\sum_{p \in Q} W'_{|a\rangle}(p, 0) = d^n W'(0, 0) = \delta_{a,0}.$$

By Eq. (28) and Theorem 6.5 it follows that  $W'(0, 0) = d^{-n}(\lambda_1 + \lambda_2 \delta_{a,0})$ , yielding  $\lambda_1 = 0$ ,  $\lambda_2 = 1$ .  $\square$

## C. Characters and Complements

Consider a space  $R = \mathbb{Z}_d^n$  with a bilinear form  $\langle \cdot, \cdot \rangle : R \times R \rightarrow \mathbb{Z}_d$ . For any  $s \in R$  the function  $r \mapsto \chi(\langle s, r \rangle)$  defines a character of  $R$ . The form is said to be *non-degenerate* if  $\langle s, \cdot \rangle \neq \langle s', \cdot \rangle$  for distinct  $s, s'$ . The two spaces we are concerned with are  $Q$  with the canonical scalar product and

$V$  with the symplectic scalar product. Both can easily be checked to be non-degenerate.

The following lemma states a basic fact about spaces with non-degenerate forms. We repeat it for completeness.

**Lemma 24.** *Let  $R = \mathbb{Z}_d^n$  with non-degenerate bilinear form  $\langle \cdot, \cdot \rangle$ . Any character  $\zeta$  of  $R$  is of the form  $\zeta(r) = \chi([s, r])$  for some unique  $s \in R$ .*

*Proof.* Addition gives  $V$  the structure of a finite abelian group. Therefore,  $V \simeq V^*$ , as is well-known (see e.g. Ref. [29]). So there are  $|V|$  different characters of  $V$ , but equally many of the form  $\chi([v, \cdot])$ .  $\square$

If  $d$  is prime and  $M$  a subspace of  $V$ , the well-known relation  $\dim M + \dim M^\perp = \dim V$  holds [36]. It is, however, no longer true in the general case. A counter-example can be constructed along the same lines as in Section II C. Still, an analogue exists as demonstrated below.

**Theorem 25.** *Let  $R = \mathbb{Z}_d^n$  with non-degenerate bilinear form  $\langle \cdot, \cdot \rangle$ . If  $M$  denotes a subspace of  $R$ , then the 'complementarity relation'  $|M| |M^\perp| = |R|$  holds.*

*Proof.* We will show that

$$M^\perp \simeq (V/M)^*. \quad (29)$$

For  $m \in M^\perp$ , the relation  $[v] \mapsto \chi([m, v])$  defines a character of  $V/M$ , as can easily be verified. Let us denote the map  $m \mapsto \chi([m, \cdot])$  by  $\iota_1$ .

Conversely, given an element  $\zeta$  of  $(V/M)^*$ ,  $v \mapsto \zeta([v])$  is a character of  $V$ . By Lemma 24 there exists a unique  $w \in V$  such that  $\zeta([v]) = \chi([w, v])$ . If  $m \in M$ , then  $\zeta([m]) = \zeta([0]) = 1$  and hence  $w \in M^\perp$ . Using the notions just introduced, we can define  $\iota_2 : (V/M)^* \rightarrow M^\perp$  by  $\zeta \mapsto w$ .

It is simple to check that  $\iota_2 = \iota_1^{-1}$ . In particular,  $\iota_1$  is invertible and Eq. (29) follows.

With the help of Lagrange's Theorem, we can compute

$$|M^\perp| = |(V/M)^*| = |V/M| = |V|/|M|,$$

which concludes the proof.  $\square$

**Corollary 26.** *Let  $V, Q$  be defined as usual. Let  $M$  be an isotropic subspace of  $V$  and  $S$  be any subspace of  $Q$ .*

1. (Maximally isotropic spaces)  *$M$  is equal to its symplectic complement  $M^\perp$  if and only if  $|M| = d^n$ .*
2. (Characters of subspaces) *Any character  $\zeta$  of  $S$  can be written as  $\zeta(s) = \chi(qs)$  for a suitable  $q \in Q$ .*

*Proof.* Claim 1 follows immediately from Theorem 25 and the fact that isotropic spaces are contained in their symplectic complement:  $M \subset M^\perp$ .

We turn to the second statement. In Lemma 14 we have argued that the characters of  $S$  which are expressible as  $\chi(qs)$  stand in one-to-one correspondence to cosets in  $Q/S^\perp$ . But  $|Q/S^\perp| = |S|$  and hence all characters are of that form.  $\square$

## D. A geometric note

The proof of the Main Theorem makes use of the fact that for any vector  $v \in V$ , there exists a symplectic operation  $S$  that sends  $v$  to a vector of the form  $(p, 0)$ . Indeed, if  $d$  is prime, any two vectors are similar, in the sense that they can be mapped onto each other by a symplectic matrix. Technically, this is a trivial incarnation of Witt's Lemma (see Ref. [37] for a formulation that is applicable in our context).

Once again the non-prime case poses additional difficulties. Recall that the *order* of a  $v \in V$  is the least positive  $\lambda \in \mathbb{Z}_d$  such that  $\lambda v = 0$ . It is easy to see that the order of a vector is left invariant by the action of invertible linear mappings. If  $d$  is a composite number (i.e. not prime), then  $V = \mathbb{Z}_d^{2n}$  contains elements of different orders which cannot be related by a linear operation. However, one might conjecture that any two vectors of equal order are similar. This is the content of the following lemma. Some concepts used in the proof can be found in Refs. [36, 38].

**Lemma 27.** (Similarity) *Let  $V = \mathbb{Z}_d^{2n}$ . Let  $a_1, a_2 \in V$  be two vectors with the same order. Then there exists a symplectic matrix  $S$  such that  $Sa_1 = a_2$ .*

*Proof.* We can slightly weaken the assumptions made about  $V$ . All we require for this proof is that  $V$  is a finite  $\mathbb{Z}_d$ -module with non-degenerate symplectic form  $[\cdot, \cdot]$ . It need not be of the form  $\mathbb{Z}_d^{2n}$ .

Let  $v \in V$  be a vector of order  $d$ . As  $v \mapsto \chi([v, \cdot])$  implements an isomorphism,  $V \rightarrow V^*$ ,  $\text{ord}(\chi([v, \cdot])) = \text{ord}(v) = d$ . There hence exists a  $w \in V$  such that  $[v, w] = \lambda$  has order  $d$ . Any such number possesses a multiplicative inverse  $\lambda^{-1}$  modulo  $\mathbb{Z}_d$  and hence  $w' = \lambda^{-1}w$  fulfills  $[v, w'] = 1$ . Vectors satisfying such a relation are said to be *hyperbolic couples*. Denote their span  $\langle \{v, w'\} \rangle$  as  $H$ .

Set  $V' := H^\perp$ . By Theorem 25  $|V| = |H| |V'|$ . Further, it is easy to see that  $H^\perp \cap H = \{0\}$  and hence  $V = H \oplus V'$ , where  $\oplus$  denotes the *orthogonal direct sum*. We claim that the symplectic inner product is non-degenerate on  $V'$ . Indeed, suppose there is a non-zero  $v' \in V'$  such that  $[v', w'] = 0$  for all  $w' \in V'$ . Then, by definition of  $V'$ ,  $[h, w'] = 0$  for all  $h \in H$  and therefore  $v'$  would be orthogonal on all vectors of  $V$ . Hence such a  $v'$  cannot exist by the non-degeneracy of  $[\cdot, \cdot]$ .

Note that  $V'$  fulfills the assumptions made about  $V$  at the beginning of the proof and has strictly smaller cardinality. Thus, we can induct on  $|V|$  to obtain a decomposition

$$V = H_1 \oplus \dots \oplus H_n$$

of  $V$  in terms of two-dimensional subspaces spanned by hyperbolic couples  $\{v_i, w'_i\}$ . We arrange these vectors as the columns of a matrix  $S = (v_1, \dots, v_n, w'_1, \dots, w'_n)$ . The construction of the couples  $\{v_i, w'_i\}$  ensures that  $S$  is symplectic, as can easily be verified.

Now let  $a_1, a_2 \in V$  be two vectors with maximal order. By the preceding discussion, there exists symplectic matrices  $S_i$  having  $a_i$  as their respective first column. Clearly, then  $S_2 S_1^{-1} a_1 = a_2$ .

Lastly, suppose  $\text{ord}(a_i) = k \leq d$ . It is easy to see that  $a'_i = ka_i/d$  are elements of  $V$  with maximal order. Further, if  $S$  maps  $a'_1$  to  $a'_2$ , then also  $a_1$  to  $a_2$ .  $\square$

**Corollary 28.** (Transitive action) *Let  $|M_1, v_1\rangle, |M_2, v_2\rangle$  be stabilizer states. If their respective associated isotropic subspaces  $M_1, M_2$  are spanned by vectors of maximal order, then there exists a Clifford operation relating these state vectors.*

*Proof.* Let  $\{m_1^{(i)}, \dots, m_n^{(i)}\}, i = 1, 2$  be bases of  $M_1$  and  $M_2$  respectively. Assume that all vectors have maximal order. It is simple to adapt the previous proof for constructing a symplectic matrix  $S$  sending  $m_i^{(1)}$  to  $m_i^{(2)}$ .  $\square$

### E. Some properties of the phase space point operators

**Lemma 29.** (Properties of the phase space point operators) *The phase space point operators fulfill the following relations*

$$\begin{aligned} A(a) &= w(2a)A(0), \\ A(a)A(b) &= w(2a - 2b), \\ \text{tr}(A(u)A(v)A(w)) &= \chi([v, u] + [u, w] + [w, v]). \end{aligned}$$

*Further, if  $U$  permutes the phase space point operators under conjugation*

$$UA(v)U^\dagger = A(v')$$

*for all  $v \in V$ , then  $U$  is Clifford.*

*Proof.* Clifford covariance (Theorem 7) implies  $A(a) = w(a)A(0)w(a)^\dagger$ . Using Theorem 6.5 it is easy to see that  $A(0)w(a)A(0) = w(-a)$  and  $A(0)^2 = 1$ . Hence

$$A(a) = w(a)A(0)w(-a)A(0)A(0) = w(2a)A(0)$$

proving the first relation. The second one follows.

For the proof of the third equation, we abbreviate  $A(0)$  as  $A$ . Then

$$\begin{aligned} &\text{tr}(A(u)A(v)A(w)) \\ &= \text{tr}(w(2u)Aw(2v)Aw(2w)A) \\ &= \text{tr}(w(2u)w(-2v)w(2w)A^3) \\ &= \chi([u, -v] + [u - v, w]) \text{tr}(w(2(u - v + w))A) \\ &= \chi([v, u] + [u, w] + [w, v]) \text{tr}(A(u - v + w)). \end{aligned}$$

It has been noted in Theorem 6.6 that phase space point operators have unit trace, which concludes the proof.

Lastly, suppose the action of  $U$  permutes phase space point operators. For any  $a \in V$ , we have

$$\begin{aligned} Uw(a)U^\dagger &= Uw(2^{-1}(a - 0))U^\dagger \\ &= UA(a)U^\dagger A(0)U^\dagger \\ &= A(a')A(0') \\ &= w(2(a' - 0')) \end{aligned}$$

for suitable  $a', 0' \in V$ . Hence  $U$  maps Weyl operators to Weyl operators and is thus Clifford by definition.  $\square$

- 
- [1] A. Kenfack, K. Życzkowski, J. Opt. B **6**, 396 (2004).
  - [2] R. L. Hudson, Rep. Math. Phys. **6**, 249 (1974).
  - [3] F. Soto and P. Claverie, J. Math. Phys. **24**, 97 (1983).
  - [4] E. Wigner, Phys. Rev. **40**, 749 (1932).
  - [5] D.F. Walls, G.J. Milburn, *Quantum Optics*. (Springer, Berlin 1994).
  - [6] G.B. Folland, *Harmonic analysis in phase space*. (Princeton Univ. Pr., Princeton, 1989).
  - [7] W. K. Wootters, Ann. Phys. NY **176**, 1 (1987).
  - [8] U. Leonhardt, Phys. Rev. A **53**, 2998 (1996).
  - [9] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).
  - [10] C. Miquel, J. P. Paz, and M. Saraceno, Phys. Rev. A **65**, 062309 (2002).
  - [11] C.A. Munoz Villegas, A. Chavez Chavez, S. Chumakov, Yu. Fofanov, A.B. Klimov, quant-ph/0307051.
  - [12] A.B. Klimov, C. Muñoz, J. Opt. B, **7**, S588 (2005).
  - [13] M. Ruzzi, D. Galetti, M.A. Machioli, J. Phys. A, **38**, 6239 (2005).
  - [14] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, R. Simon, J. Phys. (Pramana), **65**, 981 (2006).
  - [15] D. Gross, Diploma Thesis. University of Potsdam (2005). Available online at <http://gross.qipc.org>.
  - [16] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
  - [17] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, Caltech (1997). quant-ph/9705052.
  - [18] E. Knill, LANL pre-print quant-ph/9608048 (1996).
  - [19] D. Schlingemann, Quant. Inf. Comp. **4**, 287 (2004); D. Schlingemann, Dissertation Thesis, University of Braunschweig, (2005).
  - [20] M. Grassl, A. Klappenecker, and M. Röttler, *Graphs, Quadratic Forms, and Quantum Codes* in Proceedings 2002 IEEE International Symposium on Information Theory (ISIT 2002).
  - [21] E. Hostens, J. Dehaene, and B. De Moor, Phys. Rev. A, **71**, 042315 (2005).
  - [22] M. A. Nielsen, I.L. Chuang, *Quantum computation and quantum information*. (Cambridge Univ. Press, Cambridge, 2000).
  - [23] R. Raussendorf, D.E. Browne, and H.J. Briegel, Phys. Rev. A **68**, 022312 (2003).
  - [24] M. Hein, J. Eisert, and H.J. Briegel, Phys. Rev. A **69**, 062311 (2004).
  - [25] D. Gross, Appl. Phys. B. in press.
  - [26] J. Dehaene and B. De Moor, Phys. Rev. A, **68**, 042318 (2003).
  - [27] E. F. Galvao, Phys. Rev. A **71**, 042302 (2005); C. Cormick, E. F. Galvao, D. Gottesman, J. P. Paz, and A. O. Pittenger, Phys. Rev. A **73** 012301 (2006).
  - [28] A. Weil, Acta Mathematica **111**, 143 (1964).
  - [29] W. Rudin, *Fourier analysis on groups*. (Wiley-Interscience, New York, 1990).
  - [30] H. Groenewold, Physica **12**, 405 (1946).
  - [31] T. Bröcker and R. F. Werner, J. Math. Phys. **36**, 62 (1995).
  - [32] A. Pittenger and M. Rubin, J. Phys. A: Math. Gen. **38**, 6005 (2005).
  - [33] P.J. Cameron, *Classical groups*. <http://www.maths>.



qmul.ac.uk/~pjc/class\_gps/

- [34] M. Neuhauser, *Journal of Lie Theory* **12**, 15 (2002).
- [35] B. Simon, *Representations of finite and compact groups*. (American Mathematical Society, Providence, Rhode Island, 1996).
- [36] B. Huppert, *Endliche Gruppen*. (Springer, Berlin, 1967).
- [37] M. Aschbacher, *Finite group theory*. (Cambridge Univ. Press, Cambridge, 1994).
- [38] É. M. Žmud, *Math. USSR Sbornik*, **15**, 7 (1971).
- [39] T. Felbinger, *qmatrix: A Package for Quantum Information Theory*, <http://library.wolfram.com/infocenter/MathSource/1893>.
- [40] Note that the boundedness of  $\psi \in L^2(\mathbb{R}^n)$  implies that  $\theta$  has positive semi-definite imaginary part.
- [41] Up to equivalence under Clifford operations.
- [42] The choice of phase factors ensures that the symplectic inner product Eq. (5) appears in the composition law Eq. (4) thus making the connection between the Weyl operators and symplectic geometry manifest. Other definitions in use, e.g.  $w(p, q) = \hat{z}(p)\hat{x}(q)$  carry the same dependence in a less obvious manner. See also Refs. [6, 9].
- [43] Note that the “Clifford group” which appears in the context of quantum information theory [17] has no connection to the group by the same name used e.g. in the representation theory of  $SO(n)$ .
- [44] For subsets  $S$  of  $Q$ ,  $S^\perp$  denotes the *orthogonal* complement, while for subsets  $S$  of  $V$  the same symbol refers to the *symplectic* complement. This notation is natural, as for both  $Q$  and  $V$  only one respective inner product has been defined.